NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Chapter 17 Security Incident Handling and Reporting

17.1 Incident Handling and Reporting

17.1.1 NASA shall use NIST SP 800-61, Computer Security Incident Handling Guide, for additional guidance on security incident handling.

17.1.2 IT security incident response is a critical component of the NASA Information Technology Program. Incidents require close coordination among all affected NASA operations and programs to ensure that the response is appropriate.

a. The Center ITSM and incident response staff shall make a good faith effort to coordinate with system owners in determining when IT security incidents are placing NASA's missions, its customers, its reputation, or its assets in jeopardy to a degree that the Center must exercise its responsibility to unilaterally control or terminate an incident.

b. NASIRC shall continue to be the central coordination and analysis facility for incidents germane to IT security. As an authoritative repository for incident information, the NASIRC database will be used for Center and/or Agency management reports produced for internal use or external reporting.

17.1.3 An IT security incident is an adverse event or situation associated with a system that poses a threat to the integrity, availability, or confidentiality of the information or the system and results in:

a. A failure of security controls.

b. An attempted or actual compromise of information.

c. The waste, fraud, abuse, loss, or damage of Government property or information.

17.1.4 In some cases, these events may involve violations of Federal or State laws. Due to the evolving nature of laws, policies, and requirements regarding handling and reporting of information and information system incidents, detailed procedures shall be maintained by the OCIO in concert with the OIG.

17.2 Incident Handling and Reporting Requirements

17.2.1 The ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting, shall be coordinated with the OSPP and the OIG. The SOP shall conform to Federal and NIST guidance and requirements.

17.2.2 To track trends and meet Federal reporting requirements, incidents shall be categorized by the guidelines published in NIST SP 800-61, Computer Security Incident Handling Guide. The Incident Classification Framework in Figure 17-1 defines the current incident categories.

Incident Category	Definition	Clarification
Denial of Service	An explicit attack on NASA systems that prevents or impairs the authorized use of networks, systems, or applications.	Includes only those attacks that deny service to NASA systems (i.e., inbound attack on NASA systems or packet flood affecting NASA systems that was a result of malicious code).
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity (e.g., mobile code) that infects hosts at NASA.	Includes infections that result in an outbound Denial of Service attack that originates on NASA networks and attacks an external party.
Unauthorized Access	A person gains logical or physical access without permission to a NASA network, system, application,	The emphasis is on human intervention that enables access and, therefore, this category does not include malicious code that gains

	information, or other resource.	system or user privileges. These attacks will be further categorized as: System Compromise and User Compromise
Misuse	A person violates acceptable computing use policies.	
Multiple Component	An incident that falls into several incident categories at once and several exploit vulnerabilities are utilized (not just available).	A virus that creates a backdoor should be handled as a malicious code incident, not an unauthorized access incident, because the malicious code was the only transmission mechanism used. A virus that creates a backdoor that has been used to gain unauthorized access should be treated as a multiple component incident because two transmission mechanisms were used.

Figure 17-1 Incident Classification Framework

17.2.3 All NASA network, Center, program, project, and system-level procedures for detecting, reporting, and responding to IT security incidents or suspected incidents, as described in Figure 17-1, shall comply with ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.

17.2.4 All NASA contracts, cooperative agreements, grants, partnership agreements, agreements with international partners, university partners, and other educational entities, NASA Space Act Agreements, and special volunteer partners, whether funded or not funded, shall report IT security incidents and suspected incidents to the NASA sponsor and the Center ITSM. All communication about incidents transmitted between ITSMs, the CCITS Manager, Center Chiefs of Security, NASIRC, and NSOC personnel

shall be encrypted.

17.2.5 Once an incident has been confirmed, Centers shall, within two hours, provide the following information to NASIRC in an encrypted and secure manner:

a. Type of incident to include system compromise, user compromise, unauthorized access, malicious code, and denial of service.

b. An initial report containing as much information as possible including:

(1) Exploited IP addresses;

(2) Hostile IP address and domain name;

(3) Exploit used;

(4) Date and time of discovery;

(5) Date and time of exploit;

(6) Operating system with version number;

(7) Incident summary;

(8) Information types of the computers affected;

(9) Labor hours and cost of downtime; and

(10) Identification of the SSP for the exploited system.

17.2.6 The Center ITSM shall determine the incident or suspected incident's severity and potential impact on NASA's overall IT security.

a. If the Center ITSM is concerned that an incident's severity and/or potential impact on NASA's overall IT security is great, they should immediately confirm with NASIRC.

b. NASIRC should immediately notify the CCITS Manager and/or the NASA Security Operations Center (NSOC) of the incident and provide suggested remedial measures to be taken.

c. If NASIRC is not available, then the process automatically defaults to the NSOC who should continue the elevation process.

d. If the severity is suspected but not confirmed, the Center ITSM or designee must immediately seek guidance from the CCITS Manager, who will determine whether the IT security emergency process should be activated and/or strong measures are to be taken.

e. The Center ITSM shall notify the CCS and CI agent and the local OIG as soon as possible, but no later than twenty-four hours after the initial analysis.

17.2.7 Centers should populate all additional relevant fields in the NASIRC database and ensure that incidents are closed within 30 days of being reported.

a. Incidents will remain open until all information requested above is provided. Once all information has been provided, the incident will be closed.

b. Centers must provide a written justification for any incident required to remain open for more than 30 days.

c. If the justification for the extension is valid, NASIRC will present the justification to the NASA SAISO for a 30-day extension.

d. NASIRC will provide weekly updates of information not available during the preparation of the initial report.

17.2.8 Information about incidents or suspected incidents shall be handled as ACI or SBU information. IT security staff working on incidents or suspected incidents shall not disclose any information regarding inquires into incidents or suspected incidents without consent from the Center ITSM or CIO.

17.2.9 Release of incident information to those outside the NASA ITSMs, CCS, OSPP, or OIG shall be handled only by the NASA Headquarters Public Affairs Office.

17.2.10 NASIRC shall:

a. Aggregate, analyze, and provide to the Agency CIO management reports on the Center's incidents.

b. Provide insight into the nature, frequency, cost, and vector of incidents.

c. Report all IT security incidents to FedCIRC within one hour of receiving a report from a Center.

17.2.11 NASA Security Operations Center (NSOC) shall:

a. Prepare a report to improve the Center's situational awareness of hostile probe activity.

b. Provide aggregated reports to the OCIO, as directed.

17.2.12 NSOC and NASIRC shall:

a. Meet once monthly via telecom to discuss any discernable patterns and/or trends in hostile probe activity and reported incidents.

b. Discuss findings with the SAISO and, if appropriate, with the weekly ITSM teleconferences.

17.2.13 The IT Security Emergency process will be tested for after-hours notification on a quarterly basis. The test will be unannounced and will be initiated by the Manager of the CCITS.

a. NASIRC will commence the call-down within 10 minutes of the test's initiation.

b. All Centers will respond within thirty minutes of receiving NASIRC's notification.

c. The manager of the CCITS will assess NASIRC's and the Centers' responsiveness and report a pass or fail status along with their cumulative time.

17.3 Additional Security Incident Handling and Reporting References

a. NIST SP 800-61, Computer Security Incident Handling Guide.

b. NASIRC Procedures for Agency IT Security Incident Classification and Reporting.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS